

*John*



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/777,506	02/05/2001	Jeffrey Bruce Lotspiech	ARC920000143US2	8382

7590 08/04/2004  
John L. Rogitz  
Rogitz & Associates  
Suite 3120  
750 B Street  
San Diego, CA 92101

EXAMINER

CHAI, LONGBIT

ART UNIT	PAPER NUMBER
----------	--------------

2131

3

DATE MAILED: 08/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

*John*

# Office Action Summary

Application No.

09/777,506

Applicant(s)

LOTSPIECH ET AL.

Examiner

Longbit Chai

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 03 May 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☐ Claim(s) \_\_\_\_\_ is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 February 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 2.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## DETAILED ACTION

### *Priority*

1. Applicant indicates in the Priority Claim section of specification that this application is related to co-pending US patent application number 09/379,049 and claims the benefit of an earlier filing date under 35 U.S.C. 120 on 08/23/1999.
2. In fact, applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 120 as follows:
3. The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original nonprovisional application or provisional application); the disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of the first paragraph of 35 U.S.C. 112. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).
4. However, this application repeats a substantial portion of prior Application No. 09/379,049, filed on 08/23/1999, and adds and claims additional disclosure not presented in the prior application. Since this application names an inventor or inventors named in the prior application, it may constitute a continuation-in-part of the prior application. Should applicant desire to obtain the benefit of the filing date of the prior application, attention is directed to 35 U.S.C. 120 and 37 CFR 1.78.
5. As a result, the effective filing date for the subject matter defined in the pending claims 1 – 27 in this application is 02/05/2001.

***Claim Rejections - 35 USC § 102***

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 9, 10 and 11 are rejected under 35 U.S.C. 102(e) as being anticipated by Kanter (Publication Number: US 2003/0223579 A1), hereinafter referred to as Kanter.

7. As per claim 1, Kanter teaches a method for defining sets of encryption keys from a key matrix, comprising: receiving at least one parameter representing a characteristic of the key matrix; using the parameter and an error-correcting code, defining plural sets of keys; and assigning at least some sets of keys to at least some respective devices (Kanter: see for example, Paragraph [0067], Paragraph [0208] and Paragraph [0038] Line 5: Kanter teaches the key matrix is indeed the generator matrix of an error-correcting code).

8. As per claim 9, Kanter teaches A computer program device, comprising: a computer program storage device including a program of instructions usable by a computer, comprising: logic means for defining, based on at least one error-correcting code, plural sets of keys useful by respective devices for decrypting encrypted content (Kanter: see for example, Paragraph [0067], Paragraph [0208] and Paragraph [0038] Line 5).

9. As per claim 10, Kanter teaches the claimed invention as described above (see claim 9). Kanter further teaches each set represents a set of coordinates in a key matrix (Kanter: see for example, Paragraph [0208]).

10. As per claim 11, Kanter teaches the claimed invention as described above (see claim 9). Kanter further teaches logic means for associating plural sets of keys with respective devices (Kanter: see for example, Paragraph [0208] and Paragraph [0038] Line 5).

11. Claims 1 and 9 are rejected under 35 U.S.C. 102(b) as being anticipated by Matyas (Patent Number: 5200999), hereinafter referred to as Matyas.

12. As per claim 1, Matyas teaches a method for defining sets of encryption keys from a key matrix, comprising: receiving at least one parameter representing a characteristic of the key matrix; using the parameter and an error-correcting code, defining plural sets of keys; and assigning at least some sets of keys to at least some respective devices (Matyas: see for example, Column 88 Line 43, Column 88 Line 51 – 55 and Column 2 Line 50 – 60: Matyas teaches the design concept that a ciphering key can be derived from the codeword associated with error-correcting code; or in particular, the ciphering key is the codeword and thereby the key matrix is indeed the codeword matrix of the error-correcting code).

13. As per claim 9, Matyas teaches a computer program device, comprising: a computer program storage device including a program of instructions usable by a

Art Unit: 2131

computer, comprising: logic means for defining, based on at least one error-correcting code, plural sets of keys useful by respective devices for decrypting encrypted content (Matyas: see for example, Column 88 Line 43, Column 88 Line 51 – 55 and Column 2 Line 50 – 60: Matyas teaches the design concept that a ciphering key can be derived from the codeword associated with error-correcting code; or in particular, the ciphering key is the codeword and thereby the key matrix is indeed the codeword matrix of the error-correcting code).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 18 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanter (Publication Number: US 2003/0223579 A1), hereinafter referred to as Kanter, in view of Sklar (Digital Communications Fundamentals and Applications, 1988), hereinafter referred to as Sklar.

15. As per claim 18, Kanter teaches a computer programmed with instructions to cause the computer to execute method acts including: receiving, as input, at least a number "n" representing a number of columns in a key matrix and a number "N" representing a number of rows in the key matrix; defining, based at least in part on the

Art Unit: 2131

input, plural sets of keys using a non-random function (Kanter: see for example, Paragraph [0208] and Paragraph [0038] Line 5).

16. Kanter does not expressly teach each position in the key matrix being definable by a respective index, each index being associated with a respective key useful by a decryption device for decrypting encrypted content.

17. Sklar teaches that the element (or position) of the key matrix could be a non-binary code – i.e. specified as a symbol, namely, Reed-Solomon Error-Correcting Code (Sklar: see for example, Section 5.7.4 Line 1 – 6). Therefore, the position of the matrix could be changed from the binary code {0, 1} of a key to the index of a key and the symbol is indeed a key index where each index being associated with a respective ciphering key as a member of a set of device keys.

18. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sklar within the system of Kanter because Kanter discloses a method using the error-correcting code to derive the ciphering keys and Sklar teaches the element for a particular codeword associated with error-correcting code may not necessary be a binary code, and instead can be a non-binary code defined as a symbol.

19. As per claim 21, Kanter as modified teaches the claimed invention as described above (see claim 18). Kanter as modified further teaches the method executed by the computer further includes assigning at least some sets of keys to at least some respective devices (Kanter: see for example, Paragraph [0208] and Paragraph [0038] Line 5).

20. Claims 2 – 6, 12 – 15, 18 – 22 and 25 – 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas (Patent Number: 5200999), hereinafter referred to as Matyas, in view of Sklar (Digital Communications Fundamentals and Applications, 1988), hereinafter referred to as Sklar.

21. As per claim 18, Matyas teaches a computer programmed with instructions to cause the computer to execute method acts including: receiving, as input, at least a number "n" representing a number of columns in a key matrix and a number "N" representing a number of rows in the key matrix; defining, based at least in part on the input, plural sets of keys using a non-random function (Matyas: see for example, Column 88 Line 43, Column 88 Line 51 – 55 and Column 2 Line 50 – 60).

22. Matyas does not expressly teach each position in the key matrix being definable by a respective index, each index being associated with a respective key useful by a decryption device for decrypting encrypted content.

23. Sklar teaches that the element (or position) of the key matrix could be a non-binary code – i.e. specified as a symbol, namely, Reed-Solomon Error-Correcting Code (Sklar: see for example, Section 5.7.4 Line 1 – 6). Therefore, the position of the matrix could be changed from the binary code {0, 1} of a key to the index of a key and the symbol is indeed a key index where each index being associated with a respective ciphering key as a member of a set of device keys.

24. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sklar within the system of Matyas



because Matyas discloses a method using the error-correcting code to derive the ciphering keys and Sklar teaches the element for a particular codeword associated with error-correcting code may not necessary be a binary code, and instead can be a non-binary code defined as a symbol.

25. As per claim 2 and 12, Matyas teaches the claimed invention as described above (see claim 1 and 9 respectively). Matyas does not teach the error-correcting code is a Reed-Solomon code.

26. Sklar teaches the error-correcting code is a Reed-Solomon code (See same rationale addressed above in rejecting the claim 18).

27. Same rationale of combination applies herein as above in rejecting the claim 18.

28. As per claim 3, Matyas teaches the claimed invention as described above (see claim 1). Matyas does not teach each set of keys represents a set of key indices in the key matrix, each key index being associated with a respective key.

29. Sklar teaches that the element (or position) of the key matrix (or codeword matrix) could be a non-binary code – i.e. specified as a symbol, namely, Reed-Solomon Error-Correcting Code (Sklar: see for example, Section 5.7.4 Line 1 – 6). Therefore, the position of the matrix could be changed from the binary code {0, 1} of a key to the index of a key and the symbol is indeed a key index where each index being associated with a respective ciphering key as a member of a set of device keys.

30. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sklar within the system of Matyas

because Matyas discloses a method using the error-correcting code to derive the ciphering keys and Sklar teaches the element for a particular codeword associated with error-correcting code may not necessary be a binary code, and instead can be a non-binary code defined as a symbol.

31. As per claim 4 and 13, Matyas teaches the claimed invention as described above (see claim 1 and 9 respectively). Matyas does not teach the receiving act includes receiving at least a row parameter "N" representing the number of rows in the key matrix and a column parameter "n" representing the number of columns in the key matrix, and the method further includes: using an error-correcting code having a Hamming distance "d" that minimizes key overlap between sets of keys.

Sklar teaches the receiving act includes receiving at least a row parameter "N" representing the number of rows in the key matrix and a column parameter "n" representing the number of columns in the key matrix, and the method further includes: using an error-correcting code having a Hamming distance "d" that minimizes key overlap between sets of keys (i.e. the codeword matrix in particular as taught by Matyas) (Sklar: see for example, Section 5.7.4 Line 5 – 6 and Page 282 Line 4 – 8: The possible codeword should preferably be selected to provide a maximum Hamming distance between them based on the definition of hamming distance taught by Sklar).

32. As per claim 5 and 14, Matyas teaches the claimed invention as described above (see claim 4 and 13 respectively). Matyas does not teach the error-correcting code defines the sets of keys using a total predefined number "T" of sets.

33. Sklar teaches the error-correcting code defines the sets of keys using a total predefined number "T" of sets (Sklar: see for example, Section 5.7.4 Line 1 – 6: Sklar teaches each codeword has the element defined as a symbol (which is equivalent to the index of the key used in a set of device keys). Therefore, the total number sets of keys "T" would evidently equal to  $N^k$ , where N is the base of the symbol and k is the maximum number of the keys in a set of device keys – i.e. a set of device keys is considered as  $(b(1), b(2), \dots, b(k))$ , where the codeword can be simply just a key as taught by Matyas and the symbol is the key index).

34. Same rationale of combination applies herein as above in rejecting the claim 18.

35. As per claim 6, 15 and 22, Matyas teaches the claimed invention as described above (see claim 1 and 9 respectively). Matyas does not teach the error-correcting code is associated with a compact generating function and the method further comprises storing the compact generating function and an index of one and only one stored set of keys, whereby no set of keys other than the index of the stored set of keys need be stored in that sets of keys can be regenerated using the compact generating function and the index of the stored set.

36. Sklar teaches the error-correcting code is associated with a compact generating function and the method further comprises storing the compact generating function and an index of one and only one stored set of keys, whereby no set of keys other than the index of the stored set of keys need be stored in that sets of keys can be regenerated using the compact generating function and the index of the stored set (Sklar: see for example, Section 5.4.4: Sklar teaches each codeword associated with a message

vector (i.e., equivalent to the index of the stored set used herein) can be derived based on the compact generator matrix and the message vector itself (i.e., equivalent to the index of the stored set used herein as a symbol). In addition, Matyas teaches the key matrix can be simply just a codeword matrix as described above and thereby the key matrix can be derived by the compact generator matrix and the index of the stored set used herein as taught by Sklar).

37. Same rationale of combination applies herein as above in rejecting the claim 18.

38. As per claim 19, Matyas as modified teaches the claimed invention as described above (see claim 18). Matyas as modified further teaches the non-random function is an error-correcting code (Sklar: see for example, Section 5.7.4 Line 1 – 6).

39. As per claim 20, Matyas as modified teaches the claimed invention as described above (see claim 19). Matyas as modified further teaches the error-correcting code is a Reed-Solomon code (See same rationale addressed above in rejecting the claim 18).

40. As per claim 25, 26 and 27, Matyas as modified teaches the claimed invention as described above (see claim 4, 9 and 19 respectively). Matyas as modified further teaches the error-correcting code is a linear code (Sklar: see for example, Section 5.4.5).

41. Claims 8, 17 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas (Patent Number: 5200999), hereinafter referred to as Matyas, in view of Krol (Patent Number: 4512020), hereinafter referred to as Krol.

42. As per claim 8 and 17, Matyas teaches the claimed invention as described above (see claim 1 and 9 respectively). Matyas does not teach the error-correcting code generates vectors over an alphabet having symbols, and the method further comprises renaming at least one symbol based on a pseudorandom permutation.

43. Krol teaches the error-correcting code generates vectors over an alphabet having symbols, and the method further comprises renaming at least one symbol based on a pseudorandom permutation (Krol: see for example, Column 2 Line 46 – 49, and Column 7 Line 53 – 54).

44. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Krol within the system of Matyas because Matyas discloses a method using the error-correcting code to derive the ciphering keys and Krol teaches a family of error-correcting codes providing more extensive error-correcting properties (Krol: see for example, Column 1 Line 45 – 47), which also implies it would be not as obvious as being a coding method otherwise.

45. As per claim 24, Matyas as modified teaches the claimed invention as described above (see claim 18). Matyas as modified does not teach the error-correcting code generates vectors over an alphabet having symbols, and the method further comprises renaming at least one symbol based on a pseudorandom permutation.

Art Unit: 2131

46. Krol teaches the error-correcting code generates vectors over an alphabet having symbols, and the method further comprises renaming at least one symbol based on a pseudorandom permutation (Krol: see for example, Column 2 Line 46 – 49, and Column 7 Line 53 – 54).

47. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Krol within the system of Matyas as modified because Matyas as modified discloses a method using the error-correcting code to derive the ciphering keys and Krol teaches a family of error-correcting codes providing more extensive error-correcting properties (Krol: see for example, Column 1 Line 45 – 47), which also implies it would be not as obvious as being a coding pattern otherwise.

48. Claims 7, 16 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas (Patent Number: 5200999), hereinafter referred to as Matyas, in view of Crozier (Patent Number: 6145111), hereinafter referred to as Crozier, and evidenced by Krol (Patent Number: 4512020), hereinafter referred to as Krol.

49. As per claim 7, 16 and 23, Matyas as modified teaches the claimed invention as described above (see claim 6, 15 and 22 respectively). Matyas as modified does not teach the compact generating function is a generating matrix  $G$ , and the method further comprises transforming the compact generating function  $G$  to have a non-systematic row assignment.

Art Unit: 2131

50. Crozier teaches the compact generating function is a generating matrix  $G$ , and the method further comprises transforming the compact generating function  $G$  to have a non-systematic row assignment (Crozier: see for example, Column 1 Line 45 – 46, Column 6 Line 18 – 20 and Column 7 Line 6 – 9).

51. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Crozier within the system of Matyas as modified because Matyas as modified discloses a method using the error-correcting code to derive the ciphering keys and Crozier teaches a method designing high-performance and low-complexity error-correction codes.

52. Furthermore, the use of non-systematic codeword in the fields is further evidenced by Krol (Krol: see for example, Column 2 Line 46 – 47).


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai  
Examiner  
Art Unit 2131

LBC

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100